# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-099428
(43)Date of publication of application : 07.04.2000

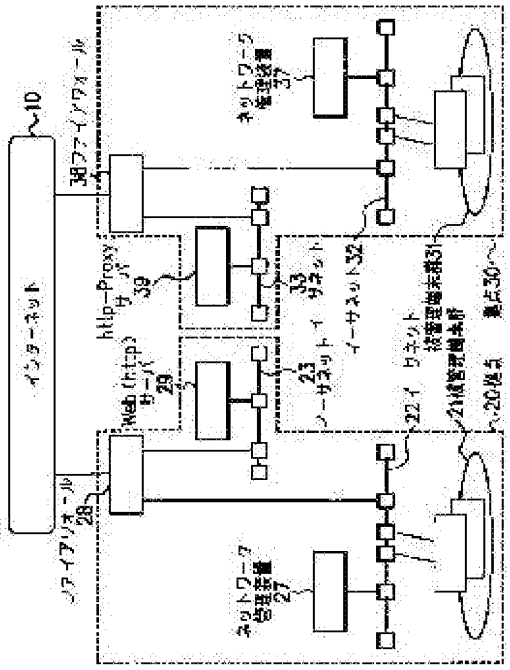
(51)Int.Cl. G06F 13/00
H04L 12/46
H04L 12/28
H04L 12/24
H04L 12/26
H04L 12/66
H04L 29/06
H04M 3/00

(21)Application number : 10-271092
(22)Date of filing : 25.09.1998

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : NAKAGAWA KENICHI
NAKAMURA NOBUTAKA

## (54) METHOD FOR COLLECTING INFORMATION BETWEEN NETWORKS AND NETWORK MANAGING DEVICE TO BE USED FOR THE SAME

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a method for collecting information on one network on the other network without changing any security condition (network policy) and a network managing device to be used for the same.
SOLUTION: A network managing device 37 acquires and stores the equipment or network information of a terminal group 31 to be managed through a managing protocol SNMP, this is assembled into HTTP protocol in order to pass it through a fire wall 38, substitutively transferred to an http-Proxy server 39 and further transferred/stored through an internet 10 into a Web (http) server 29 through an HTTP protocol, and this is acquired with the HTTP protocol by the network managing device 27 and inversely transformed to a managing protocol SNMP so that the equipment or network information of the terminal group 31 to be managed can be provided.



LEGAL STATUS

[Date of request for examination] 23.03.2000
[Date of sending the examiner's decision of rejection] 19.08.2003
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－99428
（P2000－99428A）
(43)公開日　平成12年４月７日(2000.4.7)

| (51)Int.Cl.[7] | | 識別記号 | FI | | テーマコード（参考） |
|---|---|---|---|---|---|
| Ｇ０６Ｆ | 13/00 | ３５３ | Ｃ０６Ｆ 13/00 | ３５３Ｂ | ５Ｂ０８９ |
| Ｈ０４Ｌ | 12/46 | | Ｈ０４Ｍ 3/00 | Ｂ | ５Ｋ０３０ |
| | 12/28 | | | Ｄ | ５Ｋ０３３ |
| | 12/24 | | Ｈ０４Ｌ 11/00 | ３１０Ｃ | ５Ｋ０３４ |
| | 12/26 | | 11/08 | | ５Ｋ０５１ |

審査請求　未請求　請求項の数３　ＯＬ　（全 ７ 頁）　最終頁に続く

(21)出願番号　特願平10－271092

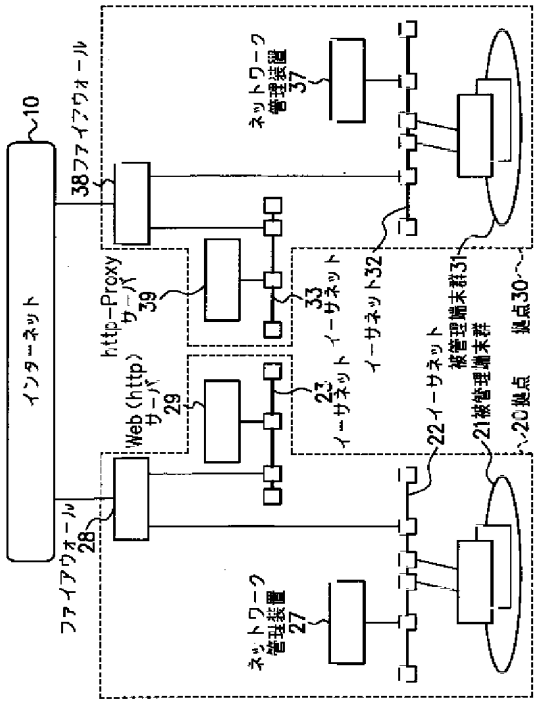
(22)出願日　平成10年９月25日(1998.9.25)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　中川　健一
東京都新宿区西新宿３丁目19番２号　日本電信電話株式会社内
(72)発明者　中村　信孝
東京都新宿区西新宿３丁目19番２号　日本電信電話株式会社内
(74)代理人　100069981
弁理士　吉田　精孝

最終頁に続く

(54)【発明の名称】　ネットワーク間における情報の収集方法及びこれに用いるネットワーク管理装置

(57)【要約】
【課題】　セキュリティ条件（ネットワークポリシー）を変更することなく、一のネットワークに関する情報を他のネットワークで収集可能とする方法及びこれに用いるネットワーク管理装置を提供すること。
【解決手段】　ネットワーク管理装置３７により被管理端末群３１の機器やネットワーク情報を管理プロトコルＳＮＭＰで取得し蓄積し、これをファイアウォール３８を疎通させるためにＨＴＴＰプロトコルに組み立て、ｈｔｔｐ－Ｐｒｏｘｙサーバ３９に代理転送し、さらにインターネット１０を介してＨＴＴＰプロトコルでＷｅｂ（ｈｔｔｐ）サーバ２９に転送・蓄積し、これをネットワーク管理装置２７によりＨＴＴＰプロトコルで取得し、管理プロトコルＳＮＭＰに逆変換して被管理端末群３１の機器やネットワーク情報を得る。



【特許請求の範囲】
【請求項１】　所定のネットワークポリシーをもって公衆ネットワークに接続される複数のネットワークのネットワーク管理装置間で情報を収集する方法において、
ネットワーク管理装置により自ネットワークに関する情報をそのネットワークポリシーの範囲内で自ネットワーク外に転送可能なプロトコルに変換し、公衆ネットワークを介して他のネットワークのネットワーク管理装置に転送することを特徴とするネットワーク間における情報の収集方法。
【請求項２】　変換するプロトコルとしてＨＴＴＰプロトコルを用いることを特徴とする請求項１記載のネットワーク間における情報の収集方法。
【請求項３】　請求項１または２記載のネットワーク間における情報の収集方法に使用されるネットワーク管理装置であって、
他のネットワークのネットワーク管理装置に転送する情報を抽出する管理データ抽出手段と、
情報抽出を行う間隔を指示するスケジューリング手段と、
管理データ抽出手段で抽出した情報を自ネットワーク外に転送可能なプロトコルに変換し、かつ他のネットワークから受信した情報のプロトコルを逆変換する転送プロトコル処理手段と、
転送プロトコル処理部とインタフェースとの間でパケットの組立及び分解を行うインタフェース制御手段とを備えたことを特徴とするネットワーク管理装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、所定のネットワークポリシーをもって公衆ネットワークに接続される複数のネットワークのネットワーク管理装置間で情報を収集する方法及びこれに用いるネットワーク管理装置に関するものである。
【０００２】
【従来の技術】図１は従来のネットワーク間における情報の収集方法を用いたシステムの一例を示すもので、図中、１は不特定多数が利用する公衆ネットワーク、２は一のネットワーク管理装置により管理されるネットワークの対象範囲（拠点）、３は他のネットワーク管理装置により管理されるネットワークの対象範囲（拠点）である。
【０００３】前記拠点２は、複数の被管理端末からなる被管理端末群２１、拠点内の各装置を接続するイーサネット２２，２３、管理プロトコルを用いて被管理端末群２１の管理情報を収集するネットワーク管理装置２４、セグメント及びポート単位にパケットの疎通許可禁止等のセキュリティ条件（ネットワークポリシー）を定義可能なファイアウォール２５、公衆ネットワーク１等からの情報を蓄積する情報蓄積サーバ２６より構成されている。
【０００４】また、拠点３は、複数の被管理端末からなる被管理端末群３１、拠点内の各装置を接続するイーサネット３２，３３、管理プロトコルを用いて被管理端末群３１の管理情報を収集するネットワーク管理装置３４、セグメント及びポート単位にパケットの疎通許可禁止等のセキュリティ条件（ネットワークポリシー）を定義可能なファイアウォール３５、イーサネット３２，３３上の機器と公衆ネットワーク１とのプロトコルを中継するプロトコル中継サーバ３６より構成されている。
【０００５】図2はファイアウォール２５，３５のセキュリティ条件により設定されるセグメント間のプロトコル疎通可否について示したもので、横軸の項目はパケットを送出（発信）するセグメント、縦軸の項目はパケットを受信（着信）するセグメントを表している。図中の記号の「○」は発信・着信セグメント間で全プロトコルの疎通を許可し、「×」は全プロトコルの疎通を禁止している。また、「Δ」は公衆ネットワーク１上の資源を利用するため、必要最低限に限定したプロトコル（ＨＴＴＰ，ＳＭＴＰ，ＮＮＴＰ等）のみの疎通を許可したものであり、内部のネットワークと公衆ネットワーク１との中継を行う。
【０００６】詳細に述べると、公衆ネットワーク１から送出されたパケットは、着信側が公衆ネットワーク１の時には全プロトコルの疎通を許可し、イーサネット２２，３２の時には全プロトコルの疎通を禁止し、イーサネット２３，３３の時には特定の中継を要するパケットのみ疎通する。
【０００７】イーサネット２２から送出されたパケットは、着信側がイーサネット２２，２３の時には全プロトコルの疎通を許可し、それ以外のセグメントに対しては全プロトコルの疎通を禁止する。イーサネット２３から送出されたパケットは、着信側がイーサネット２２，２３の時には全プロトコルの疎通を許可し、イーサネット３２の時には全プロトコルの疎通を禁止し、公衆ネットワーク１及びイーサネット３３に対しては特定の中継を要するパケットのみ疎通する。
【０００８】イーサネット３２から送出されたパケットは、着信側がイーサネット３２，３３の時には全プロトコルの疎通を許可し、それ以外のセグメントに対しては全プロトコルの疎通を禁止する。イーサネット３３から送出されたパケットは、着信側がイーサネット３２，３３の時には全プロトコルの疎通を許可し、イーサネット２２の時には全プロトコルの疎通を禁止し、公衆ネットワーク１及びイーサネット２３に対しては特定の中継を要するパケットのみ疎通する。
【０００９】
【発明が解決しようとする課題】このような従来の方法では、ネットワーク管理装置２４より公衆ネットワーク１を介して拠点３内にある、被管理端末群３１やイーサ

ネット３２上のネットワーク情報を収集し管理を行う場合、プロトコルが直接疎通可能であることが要求される。そのため、ファイアウォール２５，３５におけるイーサネット２２，３２と公衆ネットワーク１との間のセキュリティ条件（ネットワークポリシー）を、全プロトコル疎通禁止から疎通許可に変更する必要があり、新たなセキュリティホールを生じるという問題があった。

【００１０】本発明の目的は、ファイアウォール等によって定義されるセキュリティ条件（ネットワークポリシー）を変更することなく、一のネットワークに関する情報を他のネットワークで収集可能とするネットワーク間における情報の収集方法及びこれに用いるネットワーク管理装置を提供することにある。

【００１１】

【課題を解決するための手段】本発明では、前記課題を解決する方法として、所定のネットワークポリシーをもって公衆ネットワークに接続される複数のネットワークのネットワーク管理装置間で情報を収集する方法において、ネットワーク管理装置により自ネットワークに関する情報をそのネットワークポリシーの範囲内で自ネットワーク外に転送可能なプロトコルに変換し、公衆ネットワークを介して他のネットワークのネットワーク管理装置に転送することを特徴とする。

【００１２】前記構成によれば、一のネットワークに関する情報がそのネットワークポリシーの範囲内で自ネットワーク外に転送可能なプロトコルに変換され、これが公衆ネットワークを介して他のネットワークのネットワーク管理装置に転送されるため、ファイアウォール等によって定義される条件を変更することなく、任意のネットワークの管理情報が収集可能となる。

【００１３】この際、変換するプロトコルとしてＨＴＴＰプロトコルを用いることができる。

【００１４】また、このような方法は、他のネットワークのネットワーク管理装置に転送する情報を抽出する管理データ抽出手段と、情報抽出を行う間隔を指示するスケジューリング手段と、管理データ抽出手段で抽出した情報を自ネットワーク外に転送可能なプロトコルに変換し、かつ他のネットワークから受信した情報のプロトコルを逆変換する転送プロトコル処理手段と、転送プロトコル処理部とインタフェースとの間でパケットの組立及び分解を行うインタフェース制御手段とを備えたネットワーク管理装置を使用することによって実現できる。

【００１５】

【発明の実施の形態】図３は本発明のネットワーク間における情報の収集方法の実施の形態の一例を示すもので、図中、従来例と同一構成部分は同一符号をもって表す。即ち、１０は不特定多数が利用するネットワークであるインターネット、２０は一のネットワーク管理装置により管理されるネットワークの対象範囲（拠点）、３０は他のネットワーク管理装置により管理されるネットワークの対象範囲（拠点）である。

【００１６】前記拠点２０は、被管理端末群２１、イーサネット２２，２３、ネットワーク管理装置２７、ファイアウォール２８、Ｗｅｂ（ｈｔｔｐ）サーバ２９より構成されている。また、拠点３０は、被管理端末群３１、イーサネット３２，３３、ネットワーク管理装置３７、ファイアウォール３８、ｈｔｔｐ－Ｐｒｏｘｙサーバ３９より構成されている。

【００１７】ファイアウォール２８は拠点２０に対するインターネット１０からの不正接続を防止し、同拠点のセキュリティを確保する。ファイアウォール３８は拠点３０に対するインターネット１０からの不正接続を防止し、同拠点のセキュリティを確保する。

【００１８】図４はファイアウォール２８，３８のセキュリティ条件により設定されるインターネット及び各イーサネット間のプロトコル疎通可否について示したもので、横軸の項目はパケットを送出（発信）するセグメント、縦軸の項目はパケットを受信（着信）するセグメントを表している。図中の記号の「○」は発信・着信セグメント間で全プロトコルの疎通を許可し、「×」は全プロトコルの疎通を禁止している。また、「Δ」はＨＴＴＰプロトコルの疎通のみを許可し、インターネット１０上のＷｅｂ参照等のサービス提供を受けることが可能である。

【００１９】詳細に述べると、インターネット１０から送出されたパケットは、着信側がインターネット１０の時には全プロトコルの疎通を許可し、イーサネット２２，３２の時には全プロトコルの疎通を禁止し、イーサネット２３，３３の時にはＨＴＴＰプロトコルのみ疎通する。

【００２０】イーサネット２２から送出されたパケットは、着信側がイーサネット２２，２３の時には全プロトコルの疎通を許可し、それ以外のセグメントに対しては全プロトコルの疎通を禁止する。イーサネット２３から送出されたパケットは、着信側がイーサネット２２，２３の時には全プロトコルの疎通を許可し、イーサネット３２の時には全プロトコルの疎通を禁止し、インターネット１０及びイーサネット３３に対してはＨＴＴＰプロトコルのみ疎通する。

【００２１】イーサネット３２から送出されたパケットは、着信側がイーサネット３２，３３の時には全プロトコルの疎通を許可し、それ以外のセグメントに対しては全プロトコルの疎通を禁止する。イーサネット３３から送出されたパケットは、着信側がイーサネット３２，３３の時には全プロトコルの疎通を許可し、イーサネット２２の時には全プロトコルの疎通を禁止し、インターネット１０及びイーサネット２３に対してはＨＴＴＰプロトコルのみ疎通する。

【００２２】ネットワーク管理装置３７は、拠点３０に設置されている被管理端末群３１の機器情報やネットワ

ーク管理情報を管理プロトコルＳＮＭＰにより収集するとともに、ＨＴＴＰプロトコルを用いて当該情報を転送する機能を有する。ネットワーク管理装置２７は、拠点２０に設置されている被管理端末群２１の機器情報やネットワーク管理情報を管理プロトコルＳＮＭＰにより収集するとともに、ＨＴＴＰプロトコルを用いてネットワーク管理装置３７が収集した機器情報やネットワーク情報を収集し表示する機能を有する。

【００２３】Ｗｅｂ（ｈｔｔｐ）サーバ２９は、ネットワーク管理装置３７が収集した情報を蓄積することが可能であり、その接続はＨＴＴＰプロトコルによる。ｈｔｔｐ－Ｐｒｏｘｙサーバ３９はイーサネット３２上の装置がインターネット１０やＷｅｂ（ｈｔｔｐ）サーバ２９に接続を行うため、ＨＴＴＰプロトコルのパケットを中継する機能を有する。

【００２４】図５はネットワーク管理装置２７においてインターネット１０を介して被管理端末群３１に関する情報を取得する際のシーケンスを示すものである。

【００２５】ネットワーク管理装置３７は定常的に自管理下にある被管理端末群３１の機器やネットワーク情報を管理プロトコルＳＮＭＰで取得し、その情報を自装置内に蓄積・格納している。ネットワーク管理装置３７は蓄積・格納した情報をファイアウォール３８を疎通させるためにＨＴＴＰプロトコルに組み立て、ｈｔｔｐ－Ｐｒｏｘｙサーバ３９に代理転送する。

【００２６】ＨＴＴＰプロトコルで情報を受け取ったｈｔｔｐ－Ｐｒｏｘｙサーバ３９は、情報の蓄積先であるＷｅｂ（ｈｔｔｐ）サーバ２９に対してインターネット１０を介してＨＴＴＰプロトコルで転送を行う。Ｗｅｂ（ｈｔｔｐ）サーバ２９は当該情報を所定の場所に蓄積・保管する。

【００２７】ネットワーク管理装置２７は、ＨＴＴＰプロトコルでＷｅｂ（ｈｔｔｐ）サーバ２９に接続を行い、該サーバ２９上の所定の場所から情報を取得し、これを管理プロトコルＳＮＭＰに逆変換することにより、被管理端末群３１の機器やネットワーク情報を得ることができる。

【００２８】図６はネットワーク管理装置の詳細構成を示すもので、大別して既存ＮＭＳ（Ｎｅｔｗｏｒｋ　Ｍａｎａｇｅｍｅｎｔ　Ｓｙｓｔｅｍ）機能部４０と、ＮＭＳ連携機能部５０とからなり、外部とのインタフェースを介してネットワーク（イーサネット）に接続されている。

【００２９】既存ＮＭＳ機能部４０とは、従来より実現されているネットワーク管理機能を実行する部分を示しており、ネットワーク情報表示部４１、ネットワーク管理基本部４２、管理プロトコル処理部４３、インタフェース制御部４４より構成されている。

【００３０】ネットワーク情報表示部４１はネットワーク管理基本部４２の情報を画面上に表示する機能を有する。ネットワーク管理基本部４２はネットワーク上の機器等の構成や状態を監視する機能を有する。管理プロトコル処理部４３はネットワーク管理基本部４２からネットワーク上の機器等に関する情報の取得依頼を管理プロトコルに翻訳し、または取得依頼に伴う戻り値をネットワーク管理基本部４２に送信する機能を有する。インタフェース制御部４４は管理プロトコル処理部４３とインタフェースとの間でパケットへの組立及び分解を行う機能を有する。

【００３１】また、ＮＭＳ連携機能部５０とは、本発明に関わるネットワーク管理機能を実行する部分を示しており、スケジューリング部５１、管理データ抽出部５２、転送プロトコル処理部５３、インタフェース制御部５４より構成されている。

【００３２】スケジューリング部５１は管理データ抽出部５２に対して動作を行う間隔を指示する機能を有する。管理データ抽出部５２はネットワーク管理基本部４２から他のネットワーク管理装置に転送する情報を抽出し、転送プロトコル処理部５３へ送信し、また、転送プロトコル処理部５３より受信した機器等の情報をネットワーク管理基本部４２に送信する機能を有する。転送プロトコル処理部５３は管理データ抽出部５２から送出された情報を自ネットワーク外へ転送可能なプロトコルに変換し、インタフェース制御部５４に送信し、また、インタフェース制御部５４より受信した他のネットワークからの情報（管理データ）の転送プロトコルを逆変換する機能を有する。インタフェース制御部５４は転送プロトコル処理部５３とインタフェースとの間でパケットへの組立及び分解を行う機能を有する。

【００３３】

【発明の効果】以上説明したように、本発明によれば、各ネットワークにおけるセキュリティを低下させることなく、任意のネットワークにおける情報をあたかも自管理下のネットワークのように収集することが可能となる。

【図面の簡単な説明】

【図１】従来のネットワーク間における情報の収集方法の一例を示すシステム構成図

【図２】図１中のファイアウォールにおけるネットワークポリシーを示す図

【図３】本発明のネットワーク間における情報の収集方法の実施の形態の一例を示すシステム構成図

【図４】図３中のファイアウォールにおけるネットワークポリシーを示す図

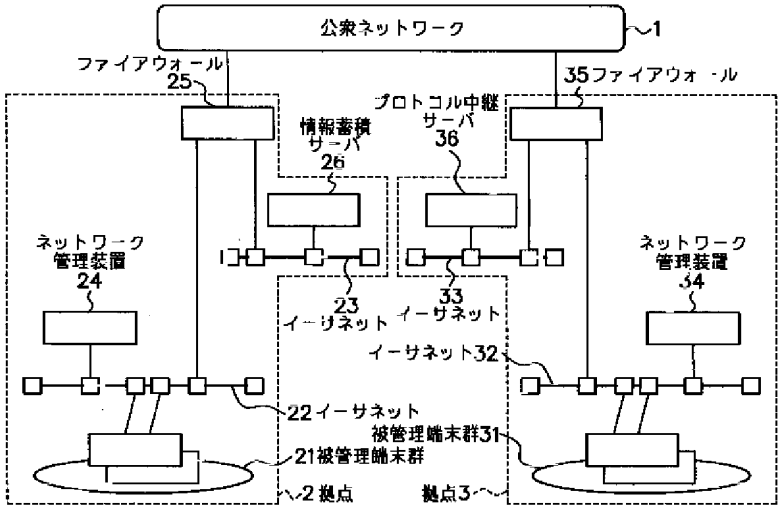
【図５】ネットワーク管理装置２７においてインターネット１０を介して被管理端末群３１に関する情報を取得する際のシーケンスを示す図

【図６】ネットワーク管理装置の詳細構成を示す機能ブロック図

【符号の説明】

１０：インターネット、２０，３０：ネットワークの対象範囲（拠点）、２１，３１：被管理端末群、２２，２３，３２，３３：イーサネット、２７，３７：ネットワーク管理装置、２８，３８：ファイアウォール、２９：Ｗｅｂ（ｈｔｔｐ）サーバ、３９：ｈｔｔｐ－ＰｒｏｘｙサーバＡ、４０：既存ＮＭＳ機能部４０、４１：ネットワーク情報表示部、４２：ネットワーク管理基本部、４３：管理プロトコル処理部、４４，５４：インタフェース制御部、５０：ＮＭＳ連携機能部、５１：スケジューリング部、５２：管理データ抽出部、５３：転送プロトコル処理部。

【図１】




【図２】

| 発 ＼ 着 | 公衆ネットワーク1 | イーサネット22 | イーサネット23 | イーサネット32 | イーサネット33 |
|---|---|---|---|---|---|
| 公衆ネットワーク1 | ○ | × | △ | × | △ |
| イーサネット22 | × | ○ | ○ | × | × |
| イーサネット23 | △ | ○ | ○ | × | △ |
| イーサネット32 | × | × | × | ○ | ○ |
| イーサネット33 | △ | × | △ | ○ | ○ |

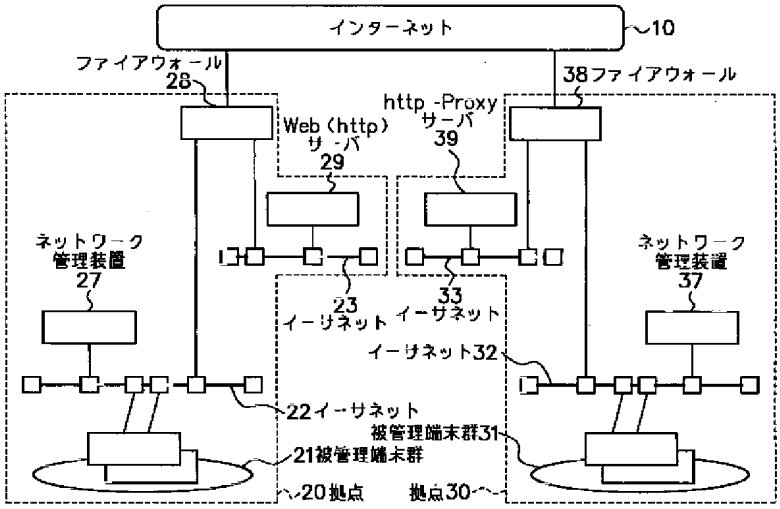
※ ○：全プロトコル疎通許可，×：全プロトコル疎通禁止，△：特定の中継プロトコル疎通許可

【図４】

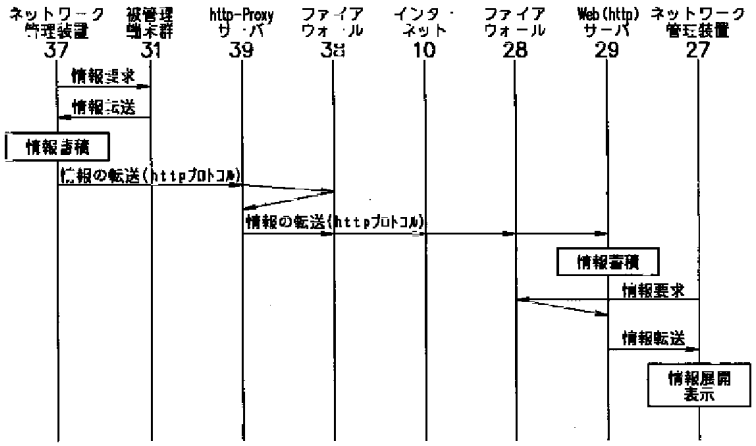
| 発 ＼ 着 | インターネット10 | イーサネット22 | イーサネット23 | イーサネット32 | イーサネット33 |
|---|---|---|---|---|---|
| インターネット10 | ○ | × | △ | × | △ |
| イーサネット22 | × | ○ | ○ | × | × |
| イーサネット23 | △ | ○ | ○ | × | △ |
| イーサネット32 | × | × | × | ○ | ○ |
| イーサネット33 | △ | × | △ | ○ | ○ |

※ ○：全プロトコル疎通許可，×：全プロトコル疎通禁止，△：HTTPプロトコル疎通許可

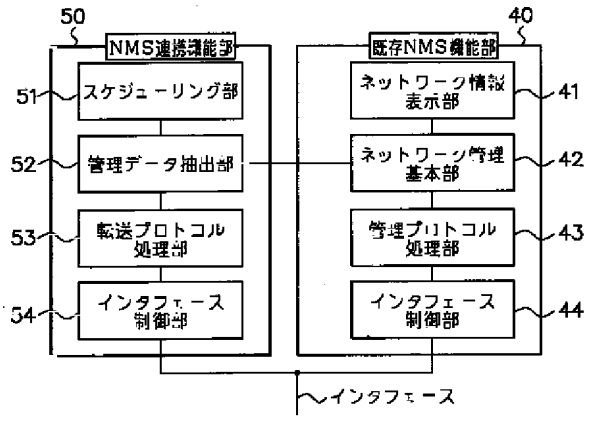
【図３】


インターネット
10
ファイアウォール
28
38ファイアウォール
http -Proxy
サーバ
39
Web (http)
サーバ
29
ネットワーク
管理装置
27
ネットワーク
管理装置
37
23
イーサネット
33
イーサネット
イーサネット32
22イーサネット
被管理端末群31
21被管理端末群
20拠点
拠点30

【図５】


ネットワーク
管理装置
37
被管理
端末群
31
http-Proxy
サーバ
39
ファイア
ウォール
38
インター
ネット
10
ファイア
ウォール
28
Web (http)
サーバ
29
ネットワーク
管理装置
27
情報要求
情報転送
情報蓄積
情報の転送(httpプロトコル)
情報の転送(httpプロトコル)
情報蓄積
情報要求
情報転送
情報展開
表示

【図６】




---

フロントページの続き

| (51)Int.Cl.[7] | 識別記号 | ＦＩ | | （参考） |
|---|---|---|---|---|
| Ｈ０４Ｌ 12/66 | | Ｈ０４Ｌ 11/20 | Ｂ | |
| 29/06 | | 13/00 | ３０５Ｃ | |
| Ｈ０４Ｍ 3/00 | | | | |

Ｆターム(参考) 5B089 GA14 GA19 GA21 GB01 HA01
HB05 HB06 JA21 KA17 KB13
KC27 KF05
5K030 HB06 HC01 HC14 HD08 JA10
LB15 MC07 MC09
5K033 BA08 BA11 BA13 CB02 CB08
CB14 DA01 DA06 DB20 EA07
5K034 AA13 AA14 EE09 HH61 HH65
MM39 QQ08 TT02
5K051 BB02 FF01